In addition, since interactions between the wallet database 1100 and the form fill systems 200a and 200b are always initiated by the wallet database 1100 acting as a "client," it is impossible for any other external system ever to get into the wallet database 1100, since that database does not accept any queries from external systems other than ones that the wallet database 1100 itself contacts in its role as a client. In addition, because the system elements do not have public internet addresses, they are neither visible nor accessible from outside the system.

[00063] For each user, the wallet database 1100 contains the non-personal identifiers or symbolic names of data elements together with the literal values of those elements which are provided by the particular user during sessions when the user accesses and updates or corrects the contents of the wallet database 1100. The method whereby the user gains access to, registers and corrects the wallet database is as follows: The user uses a User name and Password (or equivalent PIN, PKI certificate, biometric, SIM Toolkit, etc.) to access the secure server that contains all the information in their wallet. The user can access the server from a pc web browser (such as MS Internet Explorer or Netscape Navigator) or from a wireless device browser (such as the phone.com UP.browser). With the account User name and Password (or the equvalent), the wallet owner can add, modify or delete any information stored in their wallet.

[00064] Accordingly, at 1102 within the wallet database 1100, the user I.D. "JJONES" and user password "SCZTQMW" are linked to a series of non-personal or symbolic data identifiers and associated literal values. For example, the non-personal identifier or symbolic name '<FirstName>' is associated with the literal value "Jerry". In addition to such user profile data (first name, last name, address, credit card information, etc.), and while not shown in Figure 11, the wallet database for a particular user will also contain user names and passwords (PINs, etc.) that the user has, at one time or another, provided to a particular sign-on form for services such as Microsoft's Hot Mail electronic mail service or other types of services requiring user I.D.s and passwords (or PINs, etc.). As will be explained, this information is captured by the history unit 230 (Figure 9) and is stored in the wallet database entry for the user. If such a form is encountered several times, then rules are generated and added to the dictionary database 1000 and linked to the web address of that particular form, as will be explained below.

THE HISTORY DATABASE

[00065] The history database is shown at 1200. Entries in the history database 1200 are ultimately replaced by rule entries in the dictionary database 1000 when a standard rule is

applicable. The history database typically will contain information relating to two types of sites: sites with forms that have only been encountered once or possibly twice or just a limited number of times and that the system has not yet fully assimilated into the rule collection contained within the dictionary database 1000; and sites with forms that contain non-profile data unique to the specific site. A typical history database entry 1202 contains the web address of a secure fillable form followed by an indication, such as "copy 1", of which copy of the relevant information for the form this is, if several copies are stored in the history database. Linked to the form name are field labels found within the form together with the non-personal identifiers or symbolic names of data values that the history system has determined a user placed into the form at the blank locations indicated by each field name. Accordingly, if a user filled in the field labeled "Name" with the user's first name, a space, and the user's last name, then the history database will contain, linked to the web address of that form, an indication of the field label "Name" together with the wallet database symbolic names of the literal data that the user has provided. In this case, the field label "Name" would be associated with '<FirstName>" "<LastName>'. In this manner, and without invading or threatening the privacy of the personal information of any user, the history database can keep a record of forms encountered only once or twice, of their web addresses, of their field labels, and of what symbolic information a particular user has placed into those fields when filling out the form. Any data not identified as a symbolic name will be stored in the History Database 1200 as a string and used accordingly when the specific web address is encountered by the relevant user. Any data that is stored as a string is subject to future identification as a symbolic name.

THE FORM FILL SYSTEM—FILLING IN THE FORM

[00066] Figure 2 presents an overview of the form fill process, illustrating symbolically with lines the various information flow paths between the various software elements of the system and the various databases described above. The elements of the form fill system 200, which corresponds to both 200a and 200b in Figure 1, are shown enclosed within a dashed line in the central and lower portions of this Figure.

[00067] The form fill system 200 has a common entry point 202 which may be called by any client using the Internet protocol and knowing the system's Internet address. Its normal clients include the wallet SQL relational database management system (the wallet database 1100), which calls upon the system 200 to request that the wallet database 1100 be sent a request for client information, for the reasons explained above. Its other clients are one or more form fill proxies 400 (400a and 400b in Figure 1). While both the form fill proxy

400 and the wallet database 1100 call to the same common entry point 202 of the system 200, these calls are accompanied by data which distinguishes three different types of calls: those from the wallet database 1100, which are suspended until the match engine 500 or the complete form analysis engine 800 need information from the wallet database 1100; those from the form fill proxy 400 directed to the match engine 500 requesting that a form be filled out and returned; and those from the form fill proxy 400 with a completed form, reviewed and revised by the user, directed to the completed form analysis engine 800 requesting that the user reviewed and revised form be analyzed and used to improve the future operation of the form fill system 200.

[00068] With reference to Figure 2 and as explained above, the system comes into operation when a user's browser 108 or 114 receives a command from the user to download a secure form that needs to be filled out. The user's browser 108 generates an "https:// . . ." document retrieval command or its equivalent under the WAP protocol. This command is intercepted by a data flow monitor 300 (300a or 300b in Figure 1) and is routed over the path 204 to the form fill proxy 400. The form fill proxy 400 rebroadcasts this request to the vendor's web site 104 over the path 206 and receives back the server's digital I.D. which flows over the return path 208. The form fill proxy 400 verifies the identity and security of the vendor's web site 104. If the vendor's web site is not secure, the form fill proxy 400 displays a warning message to the user and terminates its activities.

[00069] If the vendor's web site is properly identified and verified, the form fill proxy 400 requests cookies from the user's browser 108 or 114 that identify the user in a way that permits access to the user's personal information in the wallet database 1100. If such cookies are present, this means that the user has previously been authenticated during the current user session, and so there is no need to query the user for an I.D. and password (or PIN, PKI certificate, etc.) at this time. The cookie request travels over the path 209 to the user's browser 108 or 114. If no cookies are found, then the form fill proxy 400 sends to the user's browser 108 or 114 over the path 210 a fill-in form requesting the user to submit a wallet user name and password (or equivalent PIN, PKI certificate, biometric, SIM Toolkit, etc.). In this manner, the form fill proxy 400 verifies the identity of the user. If the user name and password (or equivalent) are invalid, then the program terminates, displaying an appropriate error message to the user. Next, over the path 212, the form fill proxy 400 downloads, in a secure manner, the blank form from the vendor's web site 104.

[00070] The user identification information and the blank form are respectively transferred by the form fill proxy 400 over the respective paths 216 and 214 through the